PCT/JP99/05704

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年１０月１５日

出願番号
Application Number: 平成１０年特許願第３０９４１８号

出願人
Applicant (s): 三菱商事株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年１０月　１日

特許庁長官
Commissioner,
Patent Office

近藤隆彦

出証番号　出証特平１１－３０６７０

【書類名】　特許願

【整理番号】　S98033

【提出日】　平成10年10月15日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/00

【発明の名称】　２重再暗号化によりデジタルデータを保護する方法及び装置

【請求項の数】　8

【発明者】

【住所又は居所】　東京都多摩市貝取２－１２－６－１０４

【氏名】　斉藤　誠

【特許出願人】

【識別番号】　000005979

【住所又は居所】　東京都千代田区丸の内二丁目６番３号

【氏名又は名称】　三菱商事株式会社

【代理人】

【識別番号】　100099379

【弁理士】

【氏名又は名称】　南條　眞一郎

【手数料の表示】

【予納台帳番号】　027982

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【書類名】　明細書

【発明の名称】　２重再暗号化によりデジタルデータを保護する方法及び装置

【特許請求の範囲】

【請求項１】　暗号化デジタルデータを復号化し、復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを外部の可変鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の固定鍵を用いて２重に再暗号化し、２重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された２重に再暗号化された前記デジタルデータを前記内部の固定鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記外部の可変鍵を用いて２重に再復号化して利用する、デジタルデータ保護方法。

【請求項２】　暗号化デジタルデータを復号化し、　復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを内部の固定鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の可変鍵を用いて２重に再暗号化し、２重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された２重に再暗号化された前記デジタルデータを前記外部の可変鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記内部の固定鍵を用いて２重に再復号化して利用する、デジタルデータ保護方法。

【請求項３】　外部の可変鍵を用いての再暗号化及び再復号化がソフトウェアによって行われる請求項１又は２のデジタルデータ保護方法。

【請求項４】　外部の可変鍵を用いての再暗号化及び再復号化がハードウェアによって行われる請求項１又は２のデジタルデータ保護方法。

【請求項５】　暗号化デジタルデータを復号化し、復号化されたデジタルデータを利用するとともに、復号化された前記デジタルデータを外部の可変鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の固定鍵を用いて２重に再暗号化し、２重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された２重に再暗号化された前記デジタルデータを前記内部の固定鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記外部の可変鍵を用いて２重に再復号化して利用する、デジタルデータ保護装置。

【請求項６】　暗号化デジタルデータを復号化し、復号化されたデジタルデー

出証特平１１－３０６７０８１

タを利用するとともに、復号化された前記デジタルデータを内部の固定鍵を用いて再暗号化し、再暗号化された前記デジタルデータを内部の可変鍵を用いて２重に再暗号化し、２重に再暗号化された前記デジタルデータを保存あるいは転送し、保存あるいは転送された２重に再暗号化された前記デジタルデータを前記外部の可変鍵をもちいて再復号化し、再復号化された前記デジタルデータを前記内部の固定鍵を用いて２重に再復号化して利用する、デジタルデータ保護装置。

【請求項７】　外部の可変鍵を用いての再暗号化及び再復号化がソフトウェアによって行われる請求項１又は２のデジタルデータ保護方法。

【請求項８】　外部の可変鍵を用いての再暗号化及び再復号化がハードウェアによって行われる請求項１又は２のデジタルデータ保護方法。

【発明の詳細な説明】

【０００１】

【利用分野】

本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うシステムに関する。

【０００２】

【従来の技術】

従来広く普及しているアナログコンテンツは保存，複写，加工，転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。

【０００３】

デジタル映像・音声等のデジタルデータは放送，ＤＶＤ等によって有料でユーザに供給されることが多く、その場合に無料視聴を防止するために暗号化されて供給される。暗号化されて供給されたデジタルデータは何等かの手段によって供給された暗号鍵を用いて復号され、視聴される。復号されたデジタルデータは保存，複写あるいは転送を行っても品質が劣化することはないため、ユーザによっ

て保存，複写あるいは転送が行われた場合には二次的な無料視聴が行われることになり、復号されたデジタルデータコンテンツの再度の利用はコンテンツ提供者の利益に反するため、再度の利用すなわち保存，複写あるいは転送の二次利用を禁止することでシステム及び機器の開発が進められてきた。

【０００４】

しかし、二次利用を禁止することは利用者にとってはデジタルデータコンテンツの利用が魅力の乏しいものとなり、デジタルデータコンテンツの普及を阻害する要因となりかねないことが認識され、復号されたデジタルデータコンテンツの再暗号化を行うことにより不法な利用を防止するとともに、利用者にとってデジタルデータコンテンツの利用が十分に魅力あるものにすることが提案されている。

【０００５】

媒体に格納されてユーザに譲渡あるいは貸与されたデジタルデータ及びユーザに転送されたデジタルデータの保存・複写あるいは転送等の二次利用における著作権の保護は、デジタルデータがユーザの手許にあるためデジタルデータの著作権者が自ら行うことは不可能であり、何らかの方法により自動的かつ強制的に行う必要がある。

【０００６】

このような状況に鑑みて、本発明者はこれまでにデジタルコンテンツの著作権を保護することを目的としてこれまでに様々な提案を行ってきた。

本発明者らは特開平６－４６４１９号及び特開平６－１４１０００４号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【０００７】

また、特開平７－２７１８６５号及び特開平８－１８５４４８号において、デジタルコンテンツの著作権を管理するシステムについて提案した。

【０００８】

これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理セ

ンタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。

許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【０００９】

特開平７－２７１８６５号に記載されたシステムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００１０】

また、この特開平７－２７１８６５号には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存，コピー，転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【００１１】

特開平８－２８７０１４号において著作権管理を行うためのボード，ＰＣＭＣＩＡカードあるいはＩＣカードの形態を有する復号／再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

【００１２】

特開平８－２７２７４５号において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵方式と公開鍵方式を組み合わせて

加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

【００１３】

特開平８－２８８９４０号において、データベース，ビデオオンデマンド（ＶＯＤ）システムあるいは電子商取引に著作権管理システムを適用するための様々の形態を提案した。

【００１４】

特開平８－３２９０１１号において、複数データを利用・加工する場合の原データ及び新データの著作権保護を第三の暗号鍵及び著作権ラベルを用いて行うシステムを提案した。

【００１５】

以上説明した本発明者が提案してきたデータ著作権管理システム及びデータ著作権管理装置から理解されるように、データ著作権の管理は著作権管理プログラムによって暗号化／復号化／再暗号化及び利用内容の制限を行うことによって実現される。この暗号技術及び利用制限はコンピュータを使用することによって実現される。

【００１６】

さらに、ネットワークを経由して秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。

伝送時の情報窃取を暗号化により防止することが、ＵＳＰ５５０４８１８，５５１５４４１に述べられており、その場合に複数の暗号鍵を用いることがＵＳＰ５５０４８１６，５３５３３５１，５４７５７５７及び５３８１４８０に述べられており、再暗号化を行うことがＵＳＰ５４７９５１４に述べられている。

【００１７】

著作権管理プログラムによるデジタルデータの二次利用における著作権の保護は、復号されたデジタルデータの再暗号化／再復号化とこの再暗号化／再復号化を著作権管理プログラムによって管理・実行することによって実現される。

いうまでもなく、再暗号化／再復号化を行う手段としてソフトウェアウェアによるものとハードウェアによるものがある。

【００１８】

非暗号化データＭを暗号鍵Ｋを用いて暗号化データＣを得ることは、

Ｃ＝Ｅ（Ｍ，Ｋ）

という式で表現され、暗号化データＣを暗号鍵Ｋを用いて復号化データＭを得ることは、

Ｍ＝Ｄ（Ｃ，Ｋ）

という式で表現される。

【００１９】

また、復号化データＭの再暗号化／再復号化を繰り返す場合の再暗号化は、

Ｃｉ＝Ｅ（Ｄ（Ｃｉ-1，Ｋｉ-1），Ｋｉ）　　但しｉは正の整数

という式で表現され、再復号化は、

Ｍ＝Ｄ（Ｅ（Ｃｉ-1，Ｋｉ-1），Ｋｉ）

という式で表現される。

【００２０】

図１により、従来提案されているセットトップボックス（ＳＴＢ）の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット，圧縮／伸長ユニットはこの説明において省略されている。

【００２１】

この図において、１はデジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

セットトップボックス２に供給される。

【００２２】

暗号化デジタルデータＣ1を供給されたセットトップボックス２では、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センターから入手した暗号鍵Ｋ1を用い、復号化ユニット３において暗号

化デジタルデータC1を復号し、

M＝D（C1，K1）

復号化データMがディスプレイ装置４等に出力される。

【００２３】

復号化データMがデジタルビデオディスクＲＡＭ（ＤＶＤ）あるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、内蔵固定鍵方式暗号化／復号化ユニット５の再暗号化ユニット６において復号化データMがその内蔵固定鍵方式暗号化／復号化ユニット５に内蔵された固定暗号鍵K0を用いて再暗号化され、

C0＝E（M，K0）＝E（D（C1，K1），K0）

再暗号化データC0として外部装置８に保存あるいは転送される。

【００２４】

再暗号化データC0が再利用される場合には、外部装置８の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC0が内蔵固定鍵方式暗号化／復号化ユニット５の再復号化ユニット７においてその内蔵固定鍵方式暗号化／復号化ユニット５に内蔵された固定暗号鍵K0を用いて再復号化され、

M＝D（C0，K0）＝D（E（D（C1，K1），K0）

復号化データMがディスプレイ装置４等に出力される。

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データC0が保存媒体から読み出される時に保存媒体中の再暗号化データC0が消去され、再度内蔵固定暗号鍵K0を用いて再暗号化されたものが再保存されるように構成されることもある。

なお、米国特許５８０５７０６号には再暗号化／再復号化を行う集積回路が示されている。

【００２５】

このように構成されたセットトップボックスは、再暗号／再復号がハードウェアにより内蔵固定鍵K0を用いて自動的に行われるため取り扱いが容易であり、保護する必要のあるデジタルデータの強制的再暗号／再復号化には有効である。

しかし、暗号鍵Ｋ0が装置に内蔵かつ固定されているため、暗号鍵Ｋ0が知られてしまう恐れがあり、その場合には以後そのデジタルデータの保護は不可能になる。

【００２６】

【発明の概要】

この問題を解決するために、本出願では内蔵固定鍵を用いる再暗号化に加えて外部の可変鍵を用いて２重に再暗号化する方法及び装置の発明を提供する。

内蔵固定鍵と外部可変鍵の使用順には、初めに可変鍵を用い次に固定鍵を用いる場合と、初めに固定鍵を用い次に可変鍵を用いる場合とがある。

【００２７】

初めに再暗号化に用いられた鍵は後の復号化に用いられるため、後で行われた再暗号が解読された場合でも、解読に対する耐性は高い。したがって、初めに外部可変鍵を用い次に内蔵固定鍵を用いて再暗号化した場合には内蔵固定鍵が知られてしまった場合でも外部固定鍵が知られる可能性は著しく低い。

【００２８】

実施形態としてはソフトウェアによる場合とハードウェアによる場合があり、さらにソフトウェアとハードウェアの組み合わせがある。ハードウェアとしてはデジタルビデオに向けて開発された内蔵固定鍵を用いるハードウェアが利用可能である。

【００２９】

ソフトウェアによる場合プログラム及び使用される鍵の安全性を保全するためにユーザが利用することができないカーネル部以下の領域で暗号化／復号化を行う。具体的にはＩ／Ｏマネージャ内のフィルタドライバ、ディスクドライバ・ネットワークドライバであるデバイスドライバ、ＨＡＬを利用するリアルタイムＯＳで暗号化／復号化を行う。フィルタドライバはファイルシステムドライバを挟んで２つあるがどちらも利用可能であり、さらには両方を利用することも可能である。

【００３０】

【実施例】

本願発明の実施例を説明する。

図２により本発明を適用した第１実施例であるセットトップボックス（ＳＴＢ）の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

なお、この実施例のセットトップボックスにおいても図１に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット，圧縮／伸長ユニットの説明は省略されている。

【００３１】

この実施例が図１に示された従来提案されているセットトップボックスと大きく異なる点は、復号化ユニット１３と内蔵された固定鍵Ｋ0を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット１５の間にセットトップボックスの外部から供給された可変鍵Ｋ2を用いて暗号化／復号化を行う外部可変鍵方式暗号化／復号化ユニット１９が挿入されている点である。

【００３２】

この図において、１１はデジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

セットトップボックス１２に供給される。

【００３３】

暗号化デジタルデータＣ1を供給されたセットトップボックス１２では、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センタから入手した暗号鍵Ｋ1を用い、復号化ユニット１３において暗号化デジタルデータＣ1を復号し、

Ｍ＝Ｄ（Ｃ1，Ｋ1）

復号化データＭがディスプレイ装置１４等に出力される。

【００３４】

著作権主張がなされた復号化データＭが外部装置１８であるデジタルビデオデ

ィスク（ＤＶＤ）ＲＡＭあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路を経由して入手した外部可変鍵Ｋ2を用い、外部可変鍵方式暗号化／復号化ユニット１９の再暗号化ユニット２０において復号化データＭが強制的に再暗号化され、

Ｃ2＝Ｅ（Ｍ，Ｋ2）＝Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

さらに内蔵固定鍵方式暗号化／復号化ユニット１５の再再暗号化ユニット１６において再暗号化データＣ2がその内蔵固定鍵方式暗号化／復号化ユニット１５に内蔵された固定暗号鍵Ｋ0を用いて再再暗号化され、

Ｃ2-0＝Ｅ（Ｃ2，Ｋ0）＝Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

再再暗号化データＣ2-0として外部装置１８に保存あるいは転送される。

【００３５】

再再暗号化データＣ2-0が再利用される場合には、外部装置１８の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データＣ2-0が内蔵固定鍵方式暗号化／復号化ユニット１５の再復号化ユニット１７において内蔵固定鍵方式暗号化／復号化ユニット１５に内蔵された固定暗号鍵Ｋ0を用いて再復号化され、

Ｃ2＝Ｅ（Ｃ2-0，Ｋ0）＝Ｄ（Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

さらに外部可変鍵方式暗号化／復号化ユニット１９の再再復号化ユニット２１において再復号化データＣ2が暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センターから入手した外部可変鍵Ｋ2を用いて復号化され、

Ｍ＝Ｄ（Ｃ2，Ｋ2）＝Ｄ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

復号化データＭがディスプレイ装置１４等に出力される。

【００３６】

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データＣ2-0が保存媒体から読み出される時に保存媒体中の再暗号化データＣ2-0が消去され、外部可変鍵Ｋ2及び内蔵固定暗号鍵Ｋ0を用いて再暗号化されたものが再保存されるように構成されることもある。

【００３７】

このように、内蔵固定鍵を用いて再暗号化する前に外部可変鍵を用いて再暗号化する構成により、万一内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、さらに外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【００３８】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【００３９】

この実施例においては、再暗号化ユニット２０及び再再復号化ユニット２１が外部可変鍵方式暗号化／復号化ユニット１９に含まれ、再再暗号化ユニット１６及び再暗号化ユニット１７が内蔵固定鍵方式暗号化／復号化ユニット１５に含まれたものについて説明したが、これらのユニット１６，１７，２０，２１が分離して設けられても良いことは当然のことである。

【００４０】

図３により本発明を適用した第２実施例であるセットトップボックス（ＳＴＢ）の他の構成及びこのセットトップボックスで行われているデジタルデータ保護方法を説明する。

【００４１】

なお、この第２実施例のセットトップボックスにおいても図１に示された従来例のセットトップボックスの場合と同様に、暗号化／復号化と直接には関係がない周辺回路、例えば増幅ユニット，圧縮／伸長ユニットの説明は省略されている。

【００４２】

この第２実施例のセットトップボックスが図２に示された第１実施例のセットトップボックスと異なる点は、内蔵された固定鍵Ｋ0を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット３５とセットトップボックスの外部から供給された可変鍵Ｋ2を用いて暗号化／復号化を行う外部可変鍵方式暗号化

／復号化ユニット３９の挿入位置が入れ替わっている点である。

すなわち、復号化ユニット３３に内蔵された固定鍵Ｋ0を用いて暗号化／復号化を行う内蔵固定鍵方式暗号化／復号化ユニット３５が配置され、外部可変鍵Ｋ2を用いて暗号化／復号化を行う外部可変鍵方式暗号化／復号化ユニット３９が配置されている点である。

【００４３】

この図において、３１はデジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータであり、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

セットトップボックス３２に供給される。

【００４４】

暗号化デジタルデータＣ1を供給されたセットトップボックス３２では、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センタから入手した暗号鍵Ｋ1を用い、復号化ユニット３３において暗号化デジタルデータＣ1を復号し、

Ｍ＝Ｄ（Ｃ1，Ｋ1）

復号化データＭがディスプレイ装置３４等に出力される。

【００４５】

著作権主張がなされた復号化データＭが外部装置３８であるデジタルビデオディスク（ＤＶＤ）ＲＡＭあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、内蔵固定鍵方式暗号化／復号化ユニット３５の再暗号化ユニット３６において再暗号化データＣ2がその内蔵固定鍵方式暗号化／復号化ユニット３５に内蔵された固定暗号鍵Ｋ0を用いて再再暗号化され、

Ｃ0＝Ｅ（Ｍ，Ｋ0）＝Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ0）

さらに暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路を経由して入手した外部可変鍵Ｋ2を用い、外部可変鍵方式暗号化／

復号化ユニット３９の再再暗号化ユニット４０において復号化データMが強制的に再再暗号化され、

C0-2＝E（C0，K2）＝E（E（D（C1，K1），K0），K2）

再再暗号化データC0-2として外部装置３８に保存あるいは転送される。

【００４６】

再再暗号化データC0-2が再利用される場合には、外部装置３８の保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC0-2が外部可変鍵方式暗号化／復号化ユニット３９の再復号化ユニット４１において外部可変鍵K2を用いて再復号化され、

C0＝E（C0-2，K2）＝D（E（E（D（C1，K1），K0），K2）

さらに内蔵固定鍵方式暗号化／復号化ユニット３５の再再復号化ユニット３７において再復号化データC2が内蔵固定鍵方式暗号化／復号化ユニット３５に内蔵された固定暗号鍵K0を用いて再再復号化され、

M＝D（C0，K0）＝D（E（D（C1，K1），K0）

復号化データMがディスプレイ装置３４等に出力される。

【００４７】

なお、この場合安全を期するために、図中に破線で示した経路により再暗号化データC0-2が保存媒体から読み出される時に保存媒体中の再再暗号化データC0-2が消去され、内蔵固定暗号鍵K0及び外部可変鍵K2を用いて再暗号化されたものが再保存されるように構成されることもある。

【００４８】

このように、内蔵固定鍵を用いて再暗号化する前に外部可変鍵を用いて再暗号化する構成により、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、さらに外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【００４９】

また、この構成は図１に示された従来提案されているセットトップボックスの内蔵固定鍵方式暗号化／復号化ユニット３５にさらに外部可変鍵方式暗号化／復号化ユニット４１を単純に付加した構成であるから、セットトップボックスの設

計が容易である。

【００５０】

この実施例においては、再暗号化ユニット３６及び再再復号化ユニット３７が内蔵固定鍵方式暗号化／復号化ユニット３５に含まれ、再再暗号化ユニット４０及び再暗号化ユニット４１が外部可変鍵方式暗号化／復号化ユニット３９に含まれたものについて説明したが、これらのユニット３６，３７，４０，４１が分離して設けられても良いことは当然のことである。

【００５１】

デジタルデータコンテンツの取り扱いはセットトップボックスで行われるばかりでなく、パーソナルコンピュータ等のコンピュータでも行われる。

図４にから図７により、パーソナルコンピュータを用いた装置に適用した本発明の実施例を説明する。

【００５２】

パーソナルコンピュータはセットトップボックスのように全てがハードウェアで構成されハードウェアのみによって動作する装置とは異なり、装置に内蔵されたハードウェアをソフトウェアを用いて制御することによって動作する装置である。

【００５３】

コンピュータを効率的に使用するために、コンピュータの全体の動作を統括するオペレーティングシステム（ＯＳ）が用いられている。

パーソナルコンピュータ等で使用されている従来のオペレーティングシステムはメモリ管理，タスク管理，割り込み，プロセス間通信という基本的なサービスを扱うカーネル（Kernel）と、その他のサービスを扱うオペレーティングシステムサービスで構成されていた。

【００５４】

しかしながら、マイクロプロセッサの能力向上、主記憶装置として使用されるＲＡＭ価格の低下というコンピュータ側の情勢変化と、コンピュータに対する利用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシ

ステムの規模が肥大している。

【００５５】

このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

【００５６】

このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中枢サブシステムとをユーザに依存する部分であるサブシステム(Sub system)として取り除き、ハードウェアの相異を吸収するＨＡＬ(Hardware abstraction Layer)，スケジューリング機能，割り込み機能，Ｉ／Ｏ管理機能等の基本的部分をマイクロカーネル(Micro kernel)とし、サブシステムとマイクロカーネルの間にシステムサービスＡＰＩ(Application Programming Interface)を介在させてオペレーティングシステムを構成している。

【００５７】

このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。

また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

【００５８】

コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベッテッド（組み込み）用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリアルタイムオペレーティングシステムが採用されている。

【００５９】

当然のこととして組み込まれる装置毎に異なる専用のオペレーティングシステムの開発費用は大きい。　そのため、最近ではエンベデッド（組み込み）用のリアルタイムオペレーティングシステムとしてパーソナルコンピュータ用の汎用オペレーティングシステムを転用することが提案されており、マイクロカーネルと組み合わされるサブシステムにエンベデッド用の固有のプログラムを配置することにより、組み込み用のリアルタイムオペレーティングシステムを得ることが行われている。

【００６０】

オペレーティングシステムの大きな機能としてスケジューリングや割り込み処理等のタスク管理がある。

タスク管理に関して、オペレーティングシステムには大きく分けて同時に１つのタスク処理しか行わないシングルタスク方式と、同時に複数のタスク処理を行うマルチタスク方式があり、マルチタスク方式はさらにタスクの切り替えが処理されるタスクに依存するマルチタスク方式と、処理されるタスクに依存しないマルチタスク方式に区分される。

【００６１】

これらの中、シングルタスク方式はＭＰＵに１つのプロセスを割り当てそのプロセスが終了するまでＭＰＵを解放しないものであり、ノンプリエンプティブマルチタスク方式はＭＰＵを時分割して複数のプロセスに割り当てることができるが、実行中のプロセスがオペレーティングシステムに制御を戻さない限り他のプロセスは実行されないものであり、プリエンプティブマルチタスク方式はある時間間隔で実行中のプロセスに割り込みを行い、他のプロセスに強制的に制御を移すものである。

したがって、リアルタイムのマルチタスクはプリエンプティブ方式の場合にのみ可能である。

【００６２】

コンピュータにおけるタスク管理はメモリやファイルなどのシステム資源を持つ単位であるプロセスに基づいて行われ、プロセスの管理はプロセスを細分化し

たＣＰＵ時間を割り当てる単位であるスレッドに基づいて行われる。なお、この場合システム資源は同一プロセス内の全てのスレッドで共有され、したがって一つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

【００６３】

マルチタスク方式で処理される各タスクには優先順位(Priority Spectrum)があり、一般的には３２の段階に分けられる。この場合、割り込みを行わない通常のタスクは０－１５段階に分けられるダイナミッククラス(Dynamic Classes)に区分され、割り込みを行うタスクは１６－３１段階に分けられるリアルタイムクラス(Real-Time Classes)に区分される。

【００６４】

割り込み処理はタイムスライスと呼ばれる割り込み可能時間（通常１０ms）を単位として行われ通常の割り込みは１０msのタイムスライスで行われている。

このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が１００μsであるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の１０msの割り込みよりも優先して割り込みが可能である。

【００６５】

図４に示された第３実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化／復号化処理及び暗号鍵の管理は、ＨＡＬにおいてリアルタイムＯＳにより行われる。

この図において５１はコンピュータ内のオペレーティングシステム、５６はコンピュータからの出力を表示するディスプレイ装置、５７は内蔵固定鍵方式暗号化／復号化ユニット、５８はデジタルビデオディスク（ＤＶＤ）ＲＡＭあるいはハードディスク等のデータ保存媒体、又はネットワーク等のデータ転送装置である。

【００６６】

オペレーティングシステム５１はユーザ領域であるオペレーティングシステムサービス部５２，システムサービスＡＰＩ部５３，非ユーザ領域であるカーネル

５４部及びＨＡＬ５５から構成され、システムサービスＡＰＩ部５３はオペレーティングシステムサービス部５２とカーネル部５４の間に配置されて、オペレーティングシステムサービス部５２とカーネル部５４を仲介する役割を果たしており、ＨＡＬ５５はオペレーティングシステム５０の最下層に配置され、ソフトウェアから見たハードウェアハードウェアの相異を吸収する役割を担っている。

【００６７】

オペレーティングシステムサービス部５２はアプリケーション５９，サブシステム６０及びセキュリティサブシステム６１から構成され、カーネル部５４は複数のマイクロカーネルモジュール６２，６４及びカーネル６３から構成され、マイクロカーネルモジュール６２はスケジューリング，割り込み等のタスク管理機能を有し、マイクロカーネルモジュール６４はＩ／Ｏ管理機能を有する。

【００６８】

Ｉ／Ｏ管理機能を有するマイクロカーネルモジュール６４はＩ／Ｏマネージャ６５，Ｉ／Ｏマネージャに管理されるディスクドライバ６７，ネットワークドライバ６８等のデバイスドライバ及びＩ／Ｏマネージャ６５とディスクドライバ６７，ネットワークドライバ６８等のデバイスドライバとの間に必要に応じて挿入されるフィルタドライバ６６から構成されている。

【００６９】

コンピュータによる外部可変鍵方式暗号化／復号化処理はソフトウェアにより行われるが、第３実施例の場合には外部可変鍵方式暗号化／復号化処理はオペレーティングシステム５１内のＨＡＬ５５において他のタスクに優先して前に説明したリアルタイムＯＳ（ＲＴＯＳ）により行われる。

【００７０】

図２の第１実施例の場合と同様に、デジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

供給され、供給された暗号化デジタルデータＣ1は暗号化デジタルデータＣ1と同

じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センタから提供された暗号鍵Ｋ1を用いてオペレーティングシステムサービス部５２により復号され、

Ｍ＝Ｄ（Ｃ1，Ｋ1）

復号化データＭがディスプレイ装置５６等に出力される。

【００７１】

著作権主張がなされた復号化データＭがデジタルビデオディスク（ＤＶＤ）ＲＡＭあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路を経由して入手された外部可変鍵Ｋ2を用い、ＨＡＬ５５において復号化データＭが強制的に再暗号化され、

Ｃ2＝Ｅ（Ｍ，Ｋ2）＝Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

さらに内蔵固定鍵方式暗号化／復号化装置５７において再暗号化データＣ2がその内蔵固定鍵方式暗号化／復号化装置５７に内蔵された固定暗号鍵Ｋ0を用いて再再暗号化され、

Ｃ2-0＝Ｅ（Ｃ2，Ｋ0）＝Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

再再暗号化データＣ2-0として外部装置５８に保存あるいは転送される。

【００７２】

再再暗号化データＣ2-0が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データＣ2-0が内蔵固定鍵方式暗号化／復号化装置５７において内蔵された固定暗号鍵Ｋ0を用いて再復号化され、

Ｃ2＝Ｅ（Ｃ2-0，Ｋ0）＝Ｄ（Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

さらに外部可変鍵方式暗号化／復号化機能を有するＨＡＬ５５において再復号化データＣ2が暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センターから入手した外部可変鍵Ｋ2を用いて復号化され、

Ｍ＝Ｄ（Ｃ2，Ｋ2）＝Ｄ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

復号化データＭがディスプレイ装置５６等に出力される。

【００７３】

リアルタイムＯＳは他の全てのタスクに優先して実行され、この第３実施例においてはリアルタイムＯＳがオペレーティングシステムのハードウェアとの接点であるＨＡＬにおいて実行されるから、デジタルデータの再暗号化が確実に行われ、復号化データＭをそのまま外部装置５８に保存あるいは転送することは不可能となる。また、内蔵固定鍵Ｋ0を用いて再暗号化する前に外部可変鍵Ｋ2を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【００７４】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【００７５】

図５に示された第４実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化／復号化処理は、カーネル部５４内のＩ／Ｏ管理マイクロカーネルモジュール６４に挿入されたフィルタドライバ６６において行われる。

図６に示されたのは、フィルタドライバ６６が挿入されたＩ／Ｏ管理マイクロカーネルモジュール６４の構成である。

【００７６】

フィルタドライバが挿入されていないＩ／Ｏ管理マイクロカーネルモジュールは上位階層から下位階層にファイルシステムドライバ６９、中間ドライバ７０、デバイスドライバ７１が配置されており、必要に応じてファイルシステムドライバ６９の上位階層あるいは中間ドライバ７０とデバイスドライバ７１との間にフィルタドライバ６６Ａあるいはフィルタドライバ６６Ｂが挿入される。

【００７７】

これらのフィルタドライバ６６Ａ及びフィルタドライバ６６Ｂには再暗号化／再復号化処理及び暗号鍵の管理をさせることが可能であるため、この実施例にお

いては再暗号化／再復号化処理及び暗号鍵の管理をフィルタドライバ６６Ａあるいはフィルタドライバ６６Ｂに実行させる。

【００７８】

フィルタドライバはユーザが操作できるオペレーティングシステムサービス部５２ではなくユーザが操作することができないカーネル部５４に配置されている。しかし、オペレーティングシステムを使用するコンピュータに合わせて仕様を変更することが一般的に行われており、特にＩ／Ｏ管理モジュールの内容を変更することは珍しいことではない。

【００７９】

このことを利用して、第４実施例では再暗号化／再復号化処理及び暗号鍵の管理機能を有するモジュールをフィルタドライバ６６Ａあるいはフィルタドライバ６６ＢとしてＩ／Ｏ管理モジュールに挿入する。

【００８０】

図２の第１実施例の場合と同様に、デジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

供給され、供給された暗号化デジタルデータＣ1は暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センタから提供された暗号鍵Ｋ1を用いてオペレーティングシステムサービス部５２により復号され、

Ｍ＝Ｄ（Ｃ1，Ｋ1）

復号化データＭがディスプレイ装置５６等に出力される。

【００８１】

著作権主張がなされた復号化データＭがデジタルビデオディスク（ＤＶＤ）ＲＡＭあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路を経由して入手された外部可変鍵Ｋ2を用

い、フィルタドライバ６６Ａあるいは６６Ｂにおいて復号化データＭが強制的に再暗号化され、

Ｃ2＝Ｅ（Ｍ，Ｋ2）＝Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

さらに内蔵固定鍵方式暗号化／復号化装置５７において再暗号化データＣ2がその内蔵固定鍵方式暗号化／復号化装置５７に内蔵された固定暗号鍵Ｋ0を用いて再再暗号化され、

Ｃ2-0＝Ｅ（Ｃ2，Ｋ0）＝Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

再再暗号化データＣ2-0として外部装置５８に保存あるいは転送される。

【００８２】

再再暗号化データＣ2-0が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データＣ2-0が内蔵固定鍵方式暗号化／復号化装置５７において内蔵された固定暗号鍵Ｋ0を用いて再復号化され、

Ｃ2＝Ｅ（Ｃ2-0，Ｋ0）＝Ｄ（Ｅ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2），Ｋ0）

さらにフィルタドライバ６６Ａあるいは６６Ｂにおいて再復号化データＣ2が暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センターから入手した外部可変鍵Ｋ2を用いて復号化され、

Ｍ＝Ｄ（Ｃ2，Ｋ2）＝Ｄ（Ｅ（Ｄ（Ｃ1，Ｋ1），Ｋ2）

復号化データＭがディスプレイ装置５６等に出力される。

【００８３】

フィルタドライバはＩ／Ｏ管理モジュールの一部として容易にオペレーションシステムのカーネル部に挿入することができ、このようにすることにより容易にオペレーションシステムに再暗号／再復号処理及び暗号鍵の管理機能を組み込むことができる。また、内蔵固定鍵Ｋ0を用いて再暗号化する前に外部可変鍵Ｋ2を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまった場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【００８４】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使

用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【００８５】

図７に示された第５実施例では、ソフトウェアにより行われるコンピュータによる外部可変鍵方式暗号化／復号化処理及び暗号鍵管理は、オペレーティングシステム５１内のＩ／Ｏ管理マイクロカーネルモジュール６４に含まれるディスクドライバ５７及びネットワークドライバ６８において行われる。

【００８６】

図６で説明したように、Ｉ／Ｏ管理マイクロカーネルモジュールは上位階層から下位階層にファイルシステムドライバ６９、中間ドライバ７０、デバイスドライバ７１が配置されており、その最下層に位置するデバイスドライバ７１でも外部可変鍵方式暗号化／復号化処理及び暗号鍵管理を行うことができる。

【００８７】

図２の第１実施例の場合と同様に、デジタル地上波放送，デジタルＣＡＴＶ放送，デジタル衛星放送等の放送手段、インターネット等のネットワーク手段あるいはＤＶＤ，ＣＤ等のデジタル保存媒体により供給されるデジタルデータは、不正利用を防止するために暗号鍵Ｋ1を用いて暗号化されて、

Ｃ1＝Ｅ（Ｍ，Ｋ1）

供給され、供給された暗号化デジタルデータＣ1は暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路により鍵センタから提供された暗号鍵Ｋ1を用いてオペレーティングシステムサービス部５２により復号され、

Ｍ＝Ｄ（Ｃ1，Ｋ1）

復号化データＭがディスプレイ装置５６等に出力される。

【００８８】

著作権主張がなされた復号化データＭがデジタルビデオディスク（ＤＶＤ）ＲＡＭあるいはハードディスク等の媒体に保存される場合、又はネットワークを経由して外部に転送される場合は、暗号化デジタルデータＣ1と同じ経路あるいは暗号化デジタルデータＣ1と異なる経路を経由して入手された外部可変鍵Ｋ2を用

い、ディスクドライバ６７及びネットワークドライバ６８であるデバイスドライバ７１において復号化データMが強制的に再暗号化され、

C2＝E（M，K2）＝E（D（C1，K1），K2）

さらに内蔵固定鍵方式暗号化／復号化装置５７において再暗号化データC2がその内蔵固定鍵方式暗号化／復号化装置５７に内蔵された固定暗号鍵K0を用いて再再暗号化され、

C2-0＝E（C2，K0）＝E（E（D（C1，K1），K2），K0）

再再暗号化データC2-0として外部装置５８に保存あるいは転送される。

【００８９】

再再暗号化データC2-0が再利用される場合には、保存媒体から読み出されたあるいはネットワークを経由して転送された再暗号化データC2-0が内蔵固定鍵方式暗号化／復号化装置５７において内蔵された固定暗号鍵K0を用いて再復号化され、

C2＝E（C2-0，K0）＝D（E（E（D（C1，K1），K2），K0）

さらにディスクドライバ６７及びネットワークドライバ６８であるデバイスドライバ７１において再復号化データC2が暗号化デジタルデータC1と同じ経路あるいは暗号化デジタルデータC1と異なる経路により鍵センターから入手した外部可変鍵K2を用いて復号化され、

M＝D（C2，K2）＝D（E（D（C1，K1），K2）

復号化データMがディスプレイ装置５６等に出力される。

【００９０】

デバイスドライバは、オペレーティングシステムを使用するコンピュータに合わせてあるいは対象となるデバイスが改良されたような場合に仕様を変更することが極く一般的に行われている。

【００９１】

このようなデバイスドライバに再暗号／再復号処理及び暗号鍵の管理機能を組み込むこととによりオペレーションシステムのカーネル部にこれらの機能を容易に組み込むことができる。また、内蔵固定鍵K0を用いて再暗号化する前に外部可変鍵K2を用いて再暗号化することにより、もし内蔵固定鍵が知られてしまっ

た場合でもデータは外部可変鍵でも暗号化されているため、外部可変鍵を見いだして暗号化データの解読を行うことは極めて困難になる。

【００９２】

また、外部可変鍵は初めに使用され、内蔵固定鍵が使用された後に、最後に使用されるため、暗号鍵の安全性が高く、かつ初めに使用されることにより、暗号化データを最も強力に支配することになる。

【００９３】

このようにデジタルデータの再暗号化／再復号化を行うためにはそのデジタルデータの保存あるいは転送が制限されていることを識別する符号をデジタルデータに付加しておく必要がある。そして、デジタルデータが加工されることなく保存あるいは転送される場合には、これまでに述べてきた再暗号化／再復号化方法及び装置によって、デジタルデータの不正な利用を防止することができる。

【００９４】

しかし、デジタルデータに加工が行われた場合には保存あるいは転送が制限されていることを識別する符号が失われる可能性がある。

【００９５】

そのような場合には、全てのデータをその装置に固有の暗号鍵（マスターキー）を用いて再暗号化／再復号化するようにすればよい。

このようにすることにより、カット＆ペースト等の方法により加工されたデジタルデータの場合でも再暗号化／再復号化することにより不正な利用を防止することができる。

【００９６】

なお、その場合マスターキーを用いて再暗号化／再復号化するデジタルデータは保存あるいは転送が制限されていることを識別する符号が付されていないものに限定し、保存あるいは転送が制限されていることを識別する符号が付されているデジタルデータの場合にはこれまでに述べた実施例で説明した方法及び装置により再暗号化／再復号化するようにしてもよい。

【００９７】

外部可変鍵Ｋ2は何度も繰り返して使用されると知られてしまう危険性がある

。そのような場合には、特開平８－１８５４４８号公報に述べられたように暗号化使用された暗号鍵K2は廃棄され、復号に必要になったときには、再度鍵センタから入手するようにすることが適切である。

【００９８】

また、安全のためK1，K2，K0は異なる暗号アルゴリズムによるものを使用しても良い。

【図面の簡単な説明】

【図１】

従来提案されているセットトップボックスの概要構成図。

【図２】

セットトップボックスに適用したの本発明第１実施例の概要構成図。

【図３】

セットトップボックスに適用したの本発明第２実施例の概要構成図。

【図４】

パーソナルコンピュータを用いた装置に適用した本発明第３実施例の概要構成図。

【図５】

パーソナルコンピュータを用いた装置に適用した本発明第４実施例の概要構成図。

【図６】

本発明第４実施例の詳細な説明図。

【図７】

パーソナルコンピュータを用いた装置に適用した本発明第５実施例の概要構成図。

【符号の説明】

１，１１，３１　暗号化データ

２，１２，３２　セットトップボックス

３，１３，３３　復号化ユニット

４，１４，３４　ディスプレイ装置

５，１５，３５　内蔵固定鍵方式暗号化／復号化ユニット

６，２０，３６，４１　再暗号化ユニット

７，１７　再復号化ユニット

８，１８　外部装置

１６，４０　再再暗号化ユニット

１９，３９　外部可変鍵方式暗号化／復号化ユニット

２１，３７　再再復暗号化ユニット

３５，５７　内蔵固定鍵方式暗号化／復号化ユニット

４１　外部可変鍵方式暗号化／復号化ユニット

５１　オペレーティングシステム

５２　オペレーティングシステムサービス部

５３　システムサービスＡＰＩ部

５４　カーネル部

５５　ＨＡＬ

５６　ディスプレイ装置

５８　データ保存媒体・データ転送装置

５９　アプリケーション

６０　サブシステム

６１　セキュリティサブシステム

６２，６４　マイクロカーネルモジュール

６３　カーネル

６５　Ｉ／Ｏマネージャ

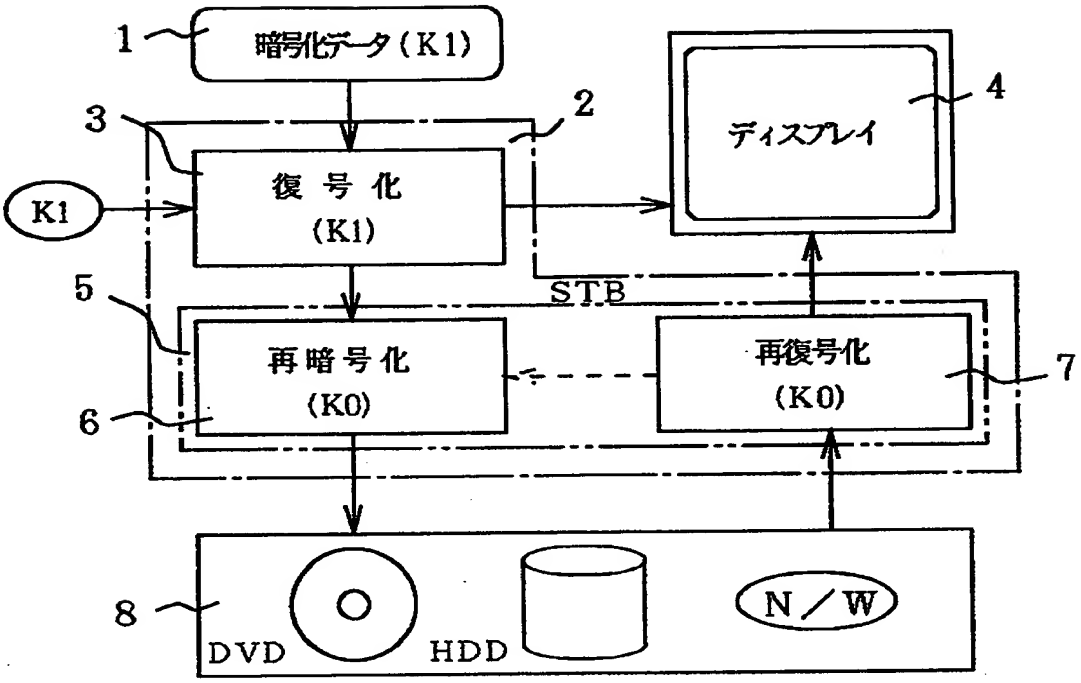
６６，６６Ａ，６６Ｂ　フィルタドライバ

６７　ディスクドライバ

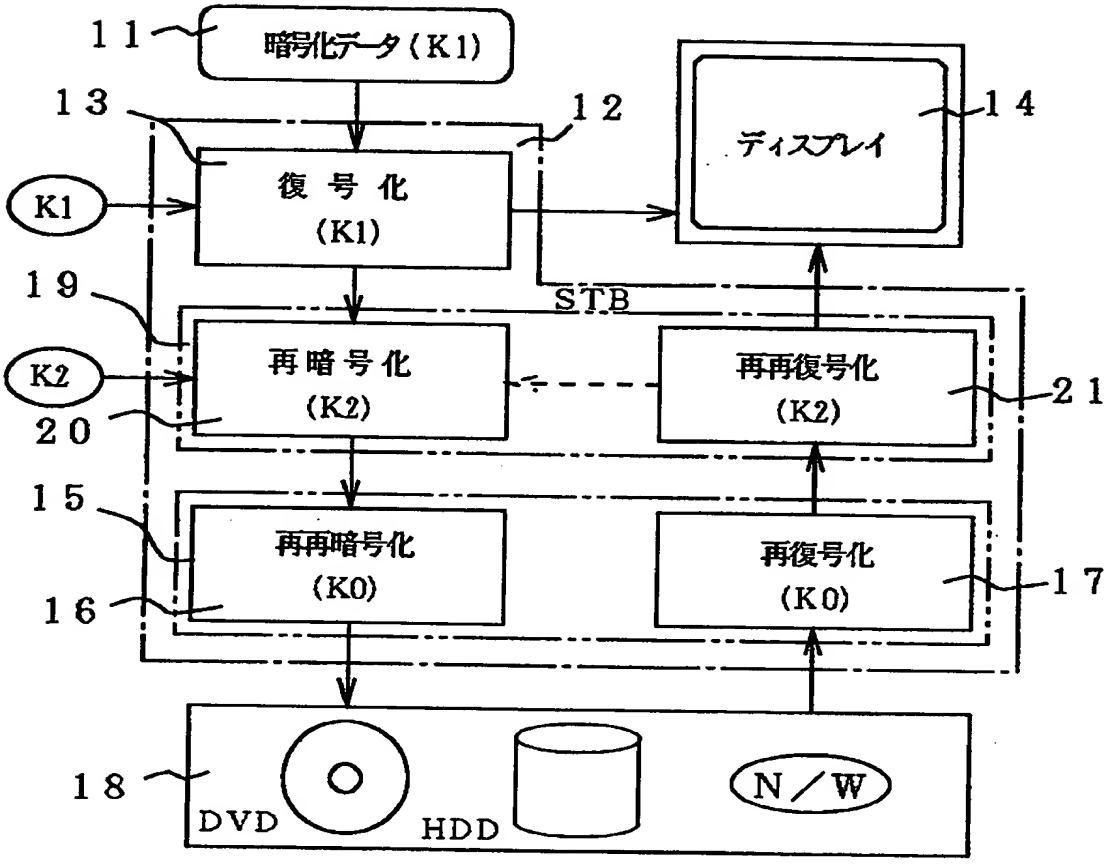
６８　ネットワークドライバ

【書類名】　図面

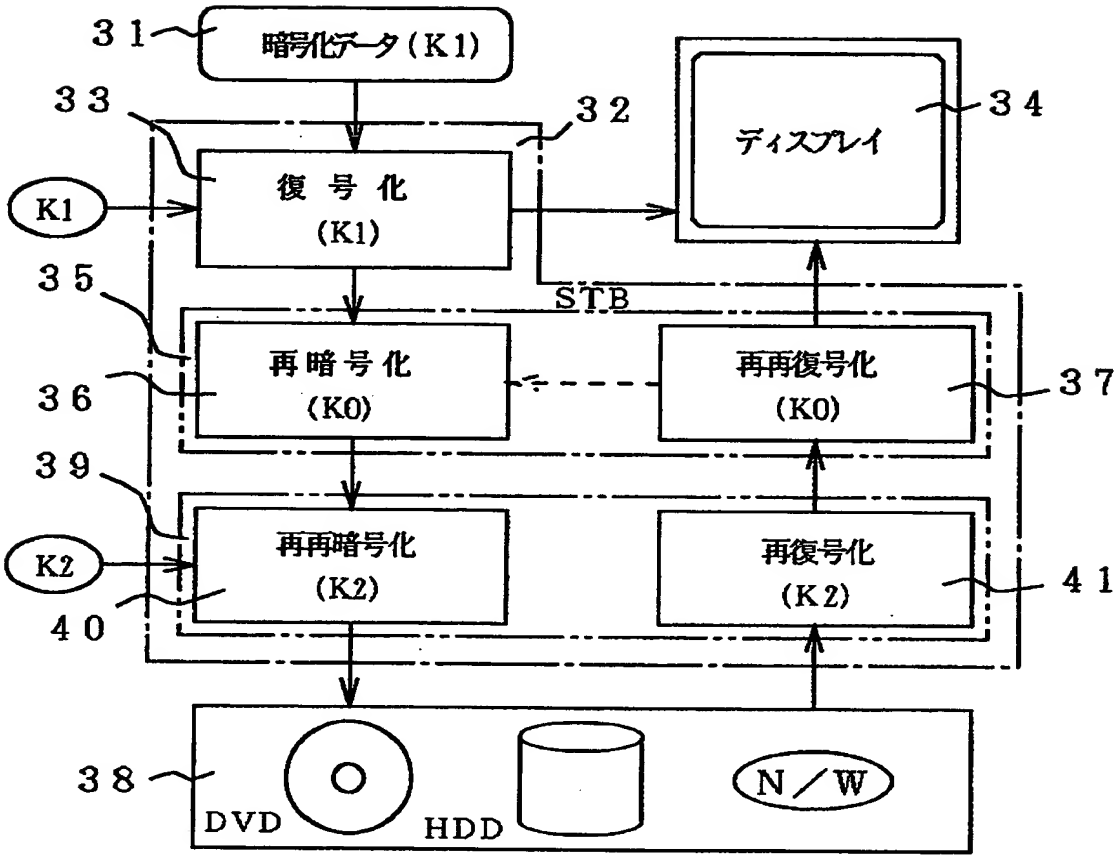
【図１】


1
暗号化データ（K1）
2
3
4
ディスプレイ
復 号 化
（K1）
K1
5
STB
再暗号化
（K0）
再復号化
（K0）
6
7
8
DVD
HDD
N／W

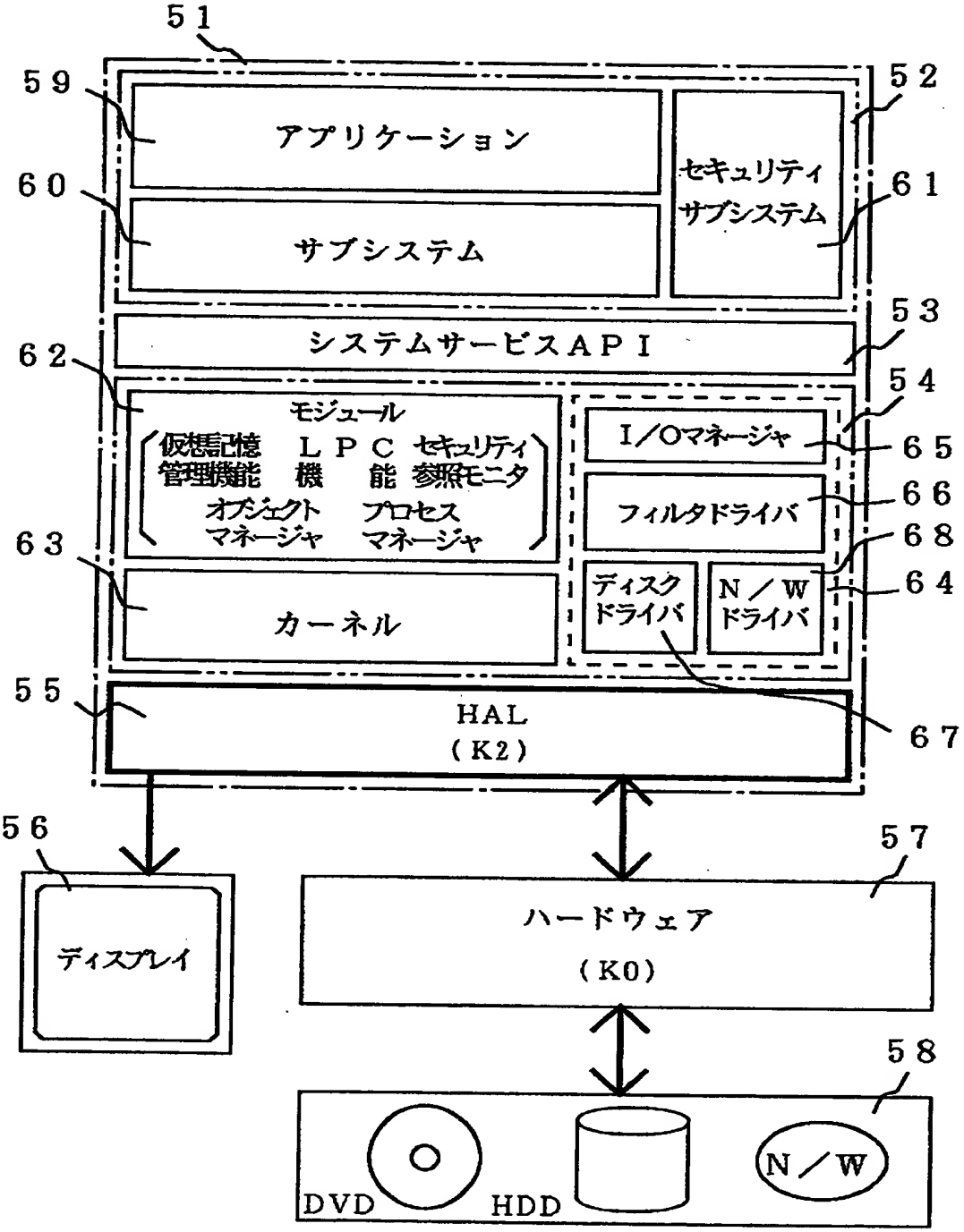
【図２】


１１
暗号化データ（K1）
１３
１２
ディスプレイ
１４
K1
復 号 化
（K1）
１９
STB
K2
再暗号化
（K2）
再再復号化
（K2）
２１
２０
１５
再再暗号化
（K0）
再復号化
（K0）
１７
１６
１８
DVD
HDD
N／W

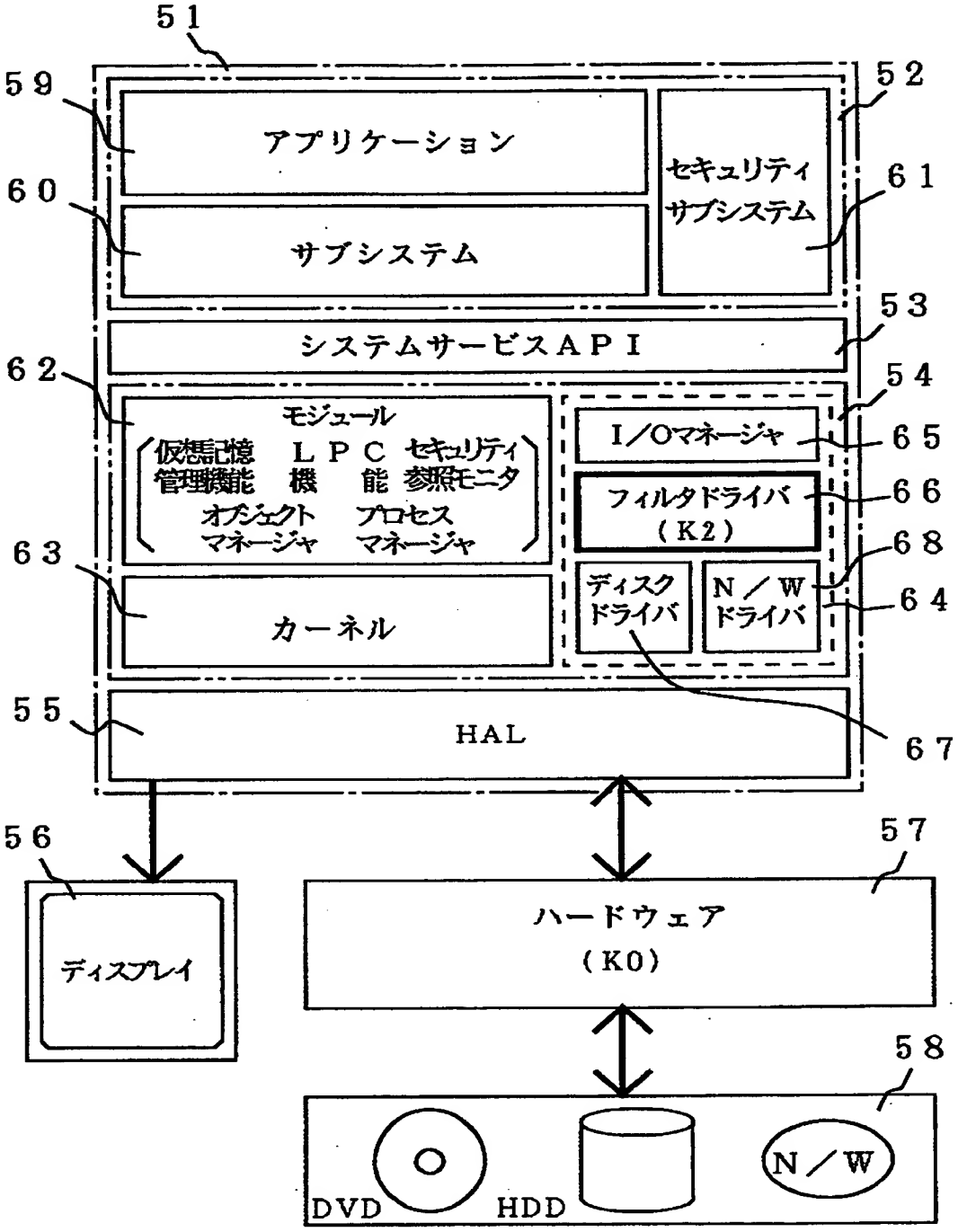
【図３】


３１
暗号化データ（K1）
３３
３２
ディスプレイ
３４
復 号 化
（K1）
K1
３５
STB
再暗号化
（K0）
再再復号化
（K0）
３７
３６
３９
再再暗号化
（K2）
再復号化
（K2）
K2
４１
４０
３８
DVD
HDD
N／W

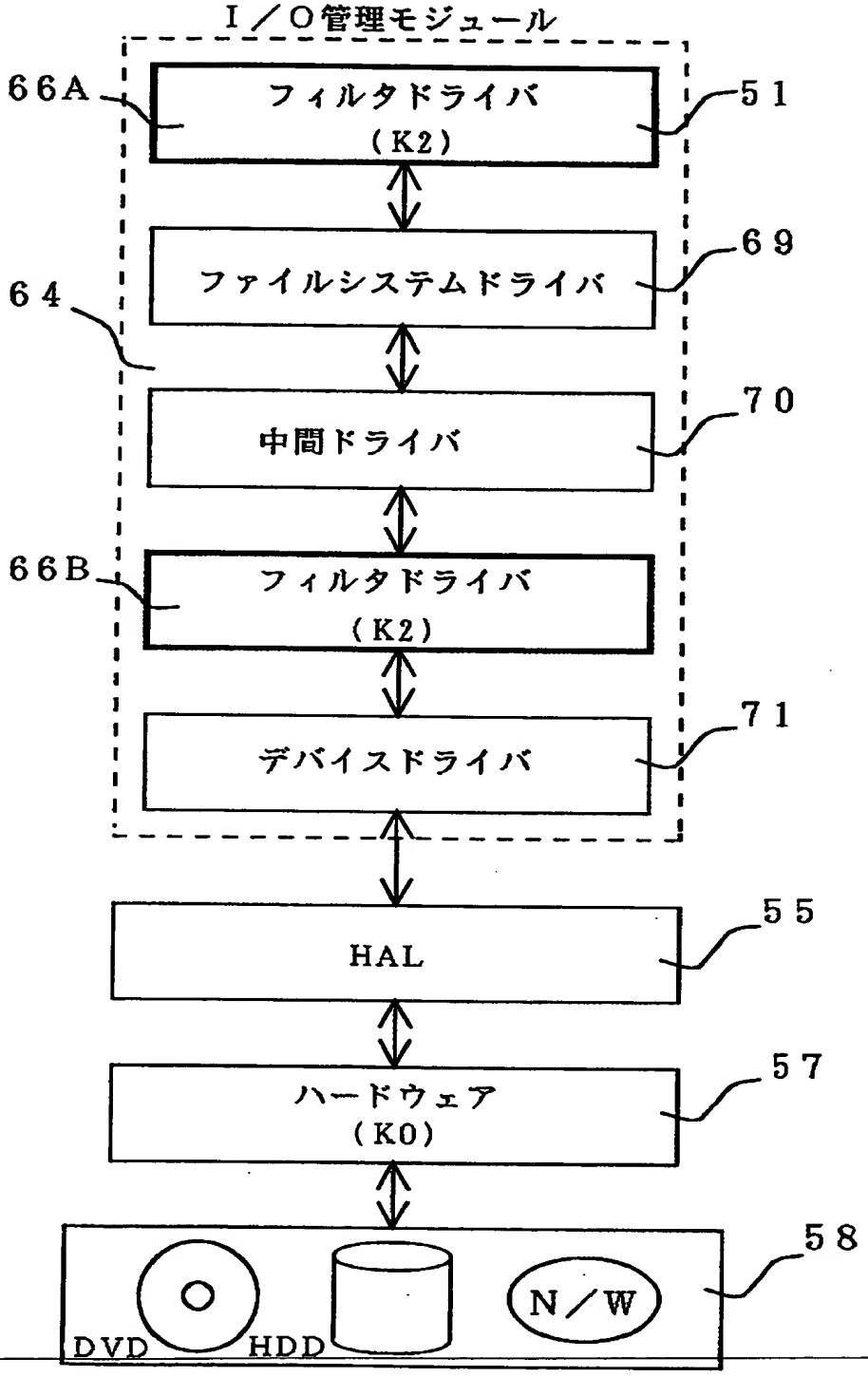
【図４】


51
59
52
アプリケーション
60
セキュリティ
サブシステム
61
サブシステム
53
システムサービスＡＰＩ
62
54
モジュール
仮想記憶 ＬＰＣ セキュリティ
管理機能 機 能 参照モニタ
オブジェクト プロセス
マネージャ マネージャ
I／Oマネージャ
65
フィルタドライバ
66
63
68
ディスク
ドライバ
N／W
ドライバ
64
カーネル
55
HAL
(K2)
67
56
57
ディスプレイ
ハードウェア
(K0)
58
DVD
HDD
N／W

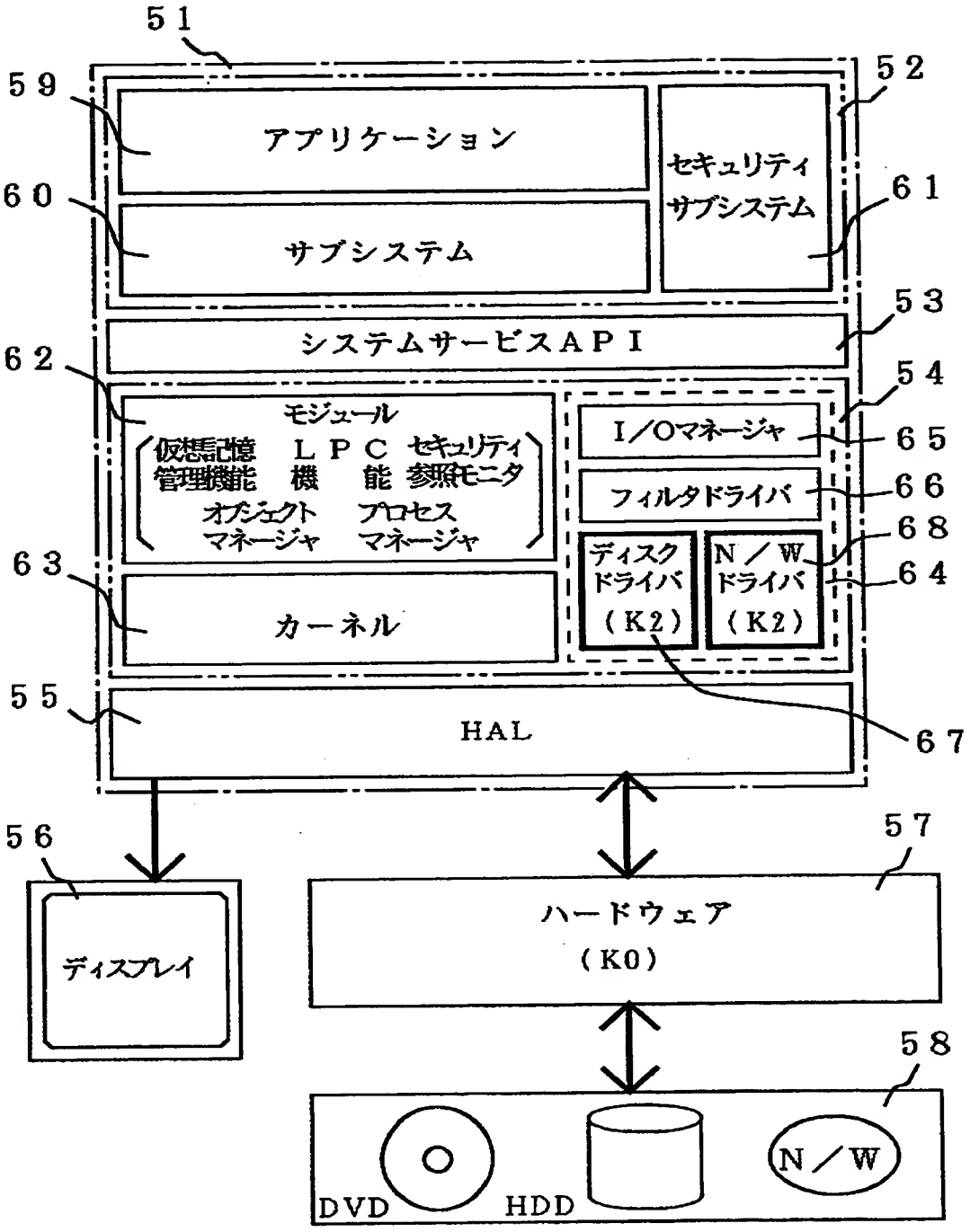
【図５】


51
52
59
アプリケーション
セキュリティ
サブシステム
61
60
サブシステム
53
システムサービスＡＰＩ
62
54
モジュール
仮想記憶 ＬＰＣ セキュリティ
管理機能 機 能 参照モニタ
オブジェクト プロセス
マネージャ マネージャ
I／Oマネージャ
65
フィルタドライバ
（K2）
66
68
63
ディスク
ドライバ
N／W
ドライバ
64
カーネル
55
HAL
67
56
57
ディスプレイ
ハードウェア
（K0）
58
DVD
HDD
N／W

【図６】


Ｉ／Ｏ管理モジュール
66A
フィルタドライバ
（K2）
51
ファイルシステムドライバ
69
64
中間ドライバ
70
66B
フィルタドライバ
（K2）
デバイスドライバ
71
HAL
55
ハードウェア
（K0）
57
DVD
HDD
N／W
58

【図７】


５１
５９
アプリケーション
５２
セキュリティ
サブシステム
６１
６０
サブシステム
５３
システムサービスＡＰＩ
６２
５４
モジュール
仮想記憶 ＬＰＣ セキュリティ
管理機能 機 能 参照モニタ
オブジェクト プロセス
マネージャ マネージャ
Ｉ／Ｏマネージャ
６５
フィルタドライバ
６６
６８
ディスク
ドライバ
（Ｋ２）
Ｎ／Ｗ
ドライバ
（Ｋ２）
６４
６３
カーネル
５５
ＨＡＬ
６７
５６
５７
ディスプレイ
ハードウェア
（Ｋ０）
５８
Ｎ／Ｗ
ＤＶＤ
ＨＤＤ

【書類名】　要約書

【要約】

【課題】　確実に再暗号化する方法及び装置を提供する。

【解決手段】　内蔵固定鍵を用いる再暗号化に加えて外部の可変鍵を用いて２重に再暗号化する。暗号鍵の使用順には、初めに可変鍵を用い次に固定鍵を用いる場合と、初めに固定鍵を用い次に可変鍵を用いる場合とがある。実施形態としてはソフトウェアによる場合とハードウェアによる場合があり、さらにソフトウェアとハードウェアの組み合わせがある。ハードウェアとしてはデジタルビデオに向けて開発された内蔵固定鍵を用いるハードウェアが利用可能である。ソフトウェアによる場合プログラム及び使用される鍵の安全性を保全するためにユーザが利用することができないカーネル部以下の領域で暗号化／復号化を行う。具体的にはＩ／Ｏマネージャ内のフィルタドライバ、ディスクドライバ・ネットワークドライバであるデバイスドライバ、ＨＡＬを利用するＲＴＯＳで暗号化／復号化を行う。フィルタドライバはファイルシステムドライバを挟んで２つあるがどちらも利用可能であり、さらには両方を利用することも可能である。

【選択図】　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005979
【住所又は居所】　東京都千代田区丸の内２丁目６番３号
【氏名又は名称】　三菱商事株式会社
【代理人】　申請人
【識別番号】　100099379
【住所又は居所】　東京都千代田区神田美土代町７番地　クボビル
【氏名又は名称】　南條　眞一郎

出　願　人　履　歴　情　報

識別番号　　〔０００００５９７９〕

１．変更年月日　　１９９０年　８月１３日
〔変更理由〕　新規登録
住　所　東京都千代田区丸の内２丁目６番３号
氏　名　三菱商事株式会社

=This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.